DEPARTMENT OF ENERGY

HEADQUARTERS

MASTER INFORMATION SYSTEMS SECURITY PLAN FOR FACSIMILE DEVICES AND DIGITAL COPIERS

October 1, 1999

Classified Information Systems Security Site Manager Approval:

/s/ Bonita S. Agee 10/01/99

Classified Information Systems Security Operations Manager Approval:

/s/ Jack Cowden 10/01/99

U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer
Office of the Associate CIO for Cyber Security
Operations Division

I

(THIS PAGE INTENTIONALLY LEFT BLANK)

Department of Energy
Headquarters
Master Information Systems Security Plan
For Facsimile Devices and Digital Copiers

INTRODUCTION

This security plan implements the requirements of DOE O 471.2A, Information Security Program, DOE M 471.2-2, Classified Information Systems Security Manual, and augments HQ Facilities Master Security Plan for the protection of classified information transmitted and received with accredited facsimile devices (Fax) or duplicated on accredited digital copiers.

The information presented in this plan is unique to stand-alone Fax devices, Digital Copiers, Optical Scanners and Multifunction Devices that offer Fax, scanner, copier and printer capabilities when operated in a stand-alone mode. When these devices are connected to and operated as personal computer peripheral devices they come under the Master Classified IS Security Plan for Personal Computers. The Master Classified Information Systems Security Plan for Fax Devices and Digital Copiers has been approved for general use; however, it alone does not fully meet the requirements for an approved security plan and cannot be used as the sole basis to gain accreditation to process classified information.

Stand-alone Fax devices and digital copiers operated under the authority of this master security plan will each be identified in the Attachment 5F, Individual Facsimile Device/Digital Copier Security Plan, which details specific system characteristics not covered in one of the subsections of this master security plan. All of the requirements in this plan supplement **must** be met. Any additions to or deviations from the requirements in this master security plan will be documented in Sections IV and V of Attachment 5F, Individual Facsimile Device/Digital Copier Security Plan.

Each Individual Security Plan must be separately approved by the Classified Information Systems Security Officer (ISSO) and forwarded to the Classified Information Security Site Manager (ISSM) with certification that it meets the requirements of the Master Classified Information Systems Security Plan for Digital Copiers & Fax Devices. The ISSM will review the Individual Security Plan, verify the ISSO's certification, and accredit the system under the authority delegated by the Classified Information Systems Security Operations Manager (ISOM).

All reorganizations which result in changes of users and/or ISSO responsibilities must immediately be brought to the attention of the ISSM so that resulting actions necessary to update the Individual Security Plans can be developed.

Fax devices and digital copiers accredited prior to the date of this plan do not have to be reaccredited under this plan until their current accreditation expires.

This document and it's Attachments are available for viewing and/or downloading from the CIO Home Page on the Internet at: **http://cio.doe.gov/compsec/**

REFERENCES

DOE O 200.1, Information Management, dated 9/30/96

DOE M 200.1-1 Telecommunications Security Manual, dated 3/1/97.

DOE O 471.2A, Information Security Program, dated 3/27/97.

DOE M 471.2-1B, Classified Matter Protection and Control Manual, dated 1/6/99.

DOE M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, dated 7/15/94, Change 1 dated 4/10/96.

DOE M 471.2-2, Classified Information Systems Security Manual, dated 8/3/99.

Headquarters Security Officer's STU-III Procedural Guide.

DOE HQ Facilities Master Security Plan, dated January 1995 with changes 1, 2, 3, 4, 5, 6, 7 and (Change 8, dated 5/3/99). **Available at http://nninfo.nn.doe.gov/**

NN-514.2 Memorandum, Subject: Deviation from the Headquarters Master Automated IS Systems Security Plan for Automated Office Support Systems, dated 2/26/96.

The DOE HQ Master Information Systems Security Plan, dated 10/1/99.

DOE Statement of Generic Threat to Information Systems, dated 2/97.

Note: DOE Orders and Manuals are available at:

http://www.explorer.doe.gov:1776/htmls/directives.html

(THIS PAGE INTENTIONALLY LEFT BLANK)

TABLE OF CONTENTS

Department of Energy
Headquarters
Master Classified Information Systems Security Plan
for Facsimile Devices and Digital Copiers

1. IDENTIFICATION AND LOCATION OF THE SYSTEM

1.1 Facility/Organization Name and Address

Headquarters
Germantown
United States Department of Energy
19901 Germantown Road
Germantown, Maryland 20874

Headquarters
Forrestal
United States Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

1.2 System Location

The specific location (where the system is installed) of each system is identified in the Individual Facsimile Device/Digital Copier Security Plan (Attachment 5F).

1.3 Accreditation Information

Fax devices and digital copiers at the HQ are individually accredited to process classified information up to, and including, the highest classification level and most restrictive category identified in Paragraph VIII-5 of the Individual Facsimile Device/Digital Copier Security Plan (Attachment 5F). Accreditation of the device referred to in the Individual Security Plan is effective upon completion of the signature of the ISSM in Paragraph VIII-4. Facsimile devices and digital copiers will be accredited for up to 18 months.

1.4 Classified Information Sensitivity Level of Concern

Level of Concern	Qualifiers
High	All SCI All Special Access Programs (SAPs)/Special Access Required (SAR) All information protecting intelligence sources, methods, and analytical procedures All Single Integrated Operational Plan (SIOP) All Crypto SECRET RD (SIGMAs 1, 2, 14, 15) TOP SECRET
Medium	SECRET SECRET RD (All other SIGMAs)
Low	CONFIDENTIAL

Note: The DAA or the data custodian may determine that additional protection measures (beyond those required by the specific level of concern) are necessary to achieve an acceptable level of risk.

2. NAME, ORGANIZATION, MAIL STOP, AND PHONE NUMBER OF THE RESPONSIBLE SECURITY PERSONNEL

2.1 Classified Information Systems Security Operations Manager (ISOM):

Jack L. Cowden, SO-213.2, GTN, (301) 903-9992

2.2 Classified Information Systems Security Site Manager (ISSM):

Bonita S. Agee, SO-322, GTN, (301) 903-4835

2.3 Headquarters Security Officer (HSO): *Attachment 5F Section I-1*

The name, organization, mail stop, and phone number of the assigned Headquarters Security Officer for your organization.

2.4 Classified Information Systems Security Officer (ISSO): *Attachment 5F Section I-2*

The name, organization, mail stop, and phone number of the assigned ISSO is provided in the applicable Individual Security Plan.

2.5 User/Security Officer (U/SO): *Attachment 5F Section I-3*

The U/SO for an accredited Fax device is the primary operator. The U/SO of an accredited Digital Copier is the key operator and/or any properly cleared staff member who has received training on the security procedures and operation of digital copiers. As such, the U/SO is responsible for complying with all IS security requirements that pertain to accredited Fax devices and/or digital copiers. The U/SO is also responsible for remaining aware of and knowledgeable about the responsibilities in regard to classified IS security. Further, U/SOs are accountable for their actions when using an accredited Fax device and/or digital copier.

(THIS PAGE INTENTIONALLY LEFT BLANK)

3. NARRATIVE DESCRIPTION OF THE IS AND ACCESS RESTRICTIONS

3.1 Purpose of the System

Accredited Fax devices allow for quick exchange of limited amounts of classified information with other organizations. Accredited Digital Copiers provide the capability to duplicate (single or multiple copies) hardcopy classified documents.

3.2 Rules for Permitting/denying Access to the Fax Device/digital Copier

U/SOs (operators) are responsible for granting access privileges to their assigned Fax device. All personnel that process classified information on accredited Fax devices must be cleared for the highest level and most restrictive category of classified information processed on the device and have signed a user responsibility acknowledgment (Attachment 1F). Accredited digital copiers may be used by any properly cleared staff member who has been trained in the security procedures and operation of digital copiers. Key Operators assigned to digital copiers have additional security responsibilities and must sign a user responsibility acknowledgment (Attachment 1F).

The specific administrative security controls implemented to deny access to uncleared personnel within the facility are listed in Paragraph 10 Administrative Security.

(THIS PAGE INTENTIONALLY LEFT BLANK)

4. STATEMENT OF THREAT

No threats unique to this system exist that were not considered and are not mitigated by the requirements and the countermeasures delineated in both DOE O 471.2A Information Security Program and DOE M 471.2-2 Classified Information Systems Security Manual.

4.1 DOE Headquarters Classified Information Systems Security Program (ISS)

Information technology (IT) advances have enabled government agencies to work more efficiently to meet their operational, financial, security and information requirements. DOE's missions in scientific research and development and nonproliferation rely heavily on IT. However, these advanced technological capabilities bring with them new security challenges. People are no longer the sole targets of collection activity. Computers and the data resident on them are now targets of criminal acts. Consequently, more and more agencies are being victimized by the actions of both employees and outsiders who exploit computer vulnerabilities. DOE's computerized systems, their related data files and the information derived from them are important DOE assets and are high priority collection targets. The increased use of IT at DOE significantly increases the risk to the confidentiality, integrity and availability of sensitive and/or classified government information/systems. (**Note:** This document supplements the ***DOE Statement of Generic Threat to Information Systems***, dated February 1997, with specific HQ information.)

4.2 Threat Factors

In order to thwart deliberate and/or malicious acts (i.e., equipment tampering, Trojan horses, virus programs, etc.) directed at classified systems, all personnel who use DOE classified ISS resources must adhere to strict security standards/procedures. Additionally, personnel must immediately report potentially damaging incidents once they become aware of the incident. By initiating these actions in a timely manner, classified users may assist in controlling and limiting the damage that may be caused by an incident. Various types of threats include:

4.2.1 ISS Incident

An adverse event associated with an ISS system(s): (a) that is a failure to comply with security regulations or directives; (b) that results in attempted, suspected, or actual compromise of classified information; or © that results in the waste, fraud, abuse, loss, or damage of government property or information.

An incident includes system contamination - processing classified information on an unclassified system.

4.2.2 Waste, Fraud or Abuse

Improper use of a DOE system/data, including: games, private use, misuse of Internet, illegal activities, personal gain, copyright violations, intentional alteration or destruction of software, hardware, or information.

4.2.3 Virus, Worms or Trojan Horse

Malicious software that is destructive or annoying in nature which attaches itself to other software that causes various results. Can be a stand-alone application designed to propagate through a network to disrupt or destroy data.

4.2.4 Trapdoor

A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner, e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions.

4.2.5 Spoofing

Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.

4.2.6 Snooping/Sniffing

Electronic monitoring of digital networks to uncover passwords or other data, and may include the visual searching for user passwords as well.

4.3 Technical Attackers

These may include all the categories of personnel previously discussed above, and a wide range of technically sophisticated computer literate personnel. Their motivation for attacking DOE systems is also wide ranging and may include: a technical challenge, righting a “perceived wrong”, denial of service, intentional harm/destruction of data, criminal activity, espionage, etc.

4.4 The Year 2000 Problem

The extensive Y2K remediation efforts currently underway in the United States also offer significant opportunities for some countries to target US Government and private sector information systems for the purpose of gaining access to critical technologies and sensitive commercial and proprietary information. Some foreign-manufactured software, or foreign experts hired to fix Y2K problems, could pose a threat to the security of sensitive information.

4.5 Headquarters Information Systems Security Threat

The Headquarters Classified ISS Program mandates a system of internal controls to safeguard DOE classified ISS assets. All computing resources at DOE are susceptible to criminal activity and unintentional or accidental threats, such as natural disaster(s), and human error(s). DOE policy is to prohibit privately owned ISS devices from entering DOE Limited and Exclusion Areas. Technological concerns include:

4.5.1 New Generation Automated Office Equipment

New generation IS equipment (i.e., video conferencing, video telephone, video E-mail, facsimile, digital copier machines, etc.) discussed below, offer the user many new capabilities that may pose serious security threats to information. The potential for unauthorized disclosure of sensitive/classified information is increased greatly when this new technology is used. Many of these technologies create potential security vulnerabilities that can be easily exploited. To further compound the problem, many of these features can be activated remotely without the knowledge of the system administrator and/or the user. Examples of new generation office technology includes:

4.5.1.1 Classified Facsimile Machines and New Generation Digital Copiers

These systems are used to transmit, receive and/or reproduce sensitive and classified information. User training is necessary to ensure the equipment is properly operated and correct precautions and sanitization procedures are taken to ensure that no sensitive/classified information is compromised.

4.5.1.2 Microphones, Video Cameras, Multimedia or Video Conferencing

It is DOE policy to ensure the secure use of these systems in areas where sensitive unclassified and/or classified information is discussed, processed, produced or displayed. It is only through this control process that inherent

technical vulnerabilities can be identified and appropriate countermeasures employed to effectively utilize this equipment without compromise.

4.5.1.3 Personal Digital Assistants

These hand-held micro-computers offer a host of features including a capability to record, transmit and/or receive information through radio frequency (RF) or infra-red (IR).

4.5.1.4 Wireless Systems

Information systems that use RF or IR to transmit and/or receive information are prohibited in Limited and Exclusion Areas.

4.5.1.5 Portable/Laptop Systems

These systems are portable and have an increased risk of theft, exploitation and/or tampering. Extra security measures must be taken if these systems are used to process classified and/or sensitive information. The extra security must protect both the hardware and data.

4.6 Countermeasures

Risk management is the integrated process of assessing the threat, vulnerabilities and the value of the protected asset, and then applying cost-effective countermeasures. The risks, threats and countermeasures must be documented in security plans to ensure the appropriate level of protection is employed to negate these threats. Training equipment users on the security safeguards is necessary to counter the risk.

4.7 Additional Information

The ISOM can assist in the conduct of risk assessments, development of countermeasures, and/or training of personnel, as necessary. Contact the HQ ISOM, (301) 903-9992 for additional information.

5. IS SECURITY ENVIRONMENT

5.1 Protection Level

The protection level for accredited Fax devices is 1 (one) as long as the operator has the required clearance and need-to-know for all of the documents processed (sent or received) through the device; otherwise the protection index changes to 2 (two). The protection index for accredited digital copiers is 1 (one). Any Fax Device or digital copier with a protection index greater than 3 (three) requires that a separate security plan be developed addressing those requirements.

5.2 Methods Used

The methods used to meet the above requirements will be described in Paragraphs 6 through 10 of this Plan. **All security measures identified in this Plan must be implemented. (All deviations must be identified in Section V of the Attachment 5F. Any security measures implemented in addition to those mentioned in this plan must be identified in Section IV of the Attachment 5F.**

5.3 Individual System Description

Individual Security Plans describe each Fax device/digital copier and identify the level and approximate amount of classified data to be processed and any special handling caveats. Fax devices/digital copiers are included in each HQ organization's property accounting inventory. Each Individual Security Plan for Fax Devices/Digital Copiers will list the following information:

a. System Identification Number, as assigned by the ISSM during the initial accreditation.
b. Location
   - Area, Building, Room
   - Responsible organization, security officials (e.g., HSO, ISSO)
c. Hardware
   - Manufacturer of the equipment
   - Model Identification
   - DOE Property Tag Number
   - STU-III Manufacturer (Fax devices only)
   - STU-III Telephone Number (Fax devices only)

5.4 System Security Testing

Each Fax device and digital copier installation is separately accredited and, as part of the accreditation process, is reviewed for compliance with this Master IS Security Plan for Facsimile Devices and Digital Copiers and its associated Individual Security Plan.

Attachment 4F presents a brief security compliance checklist that is used as an aid in the compliance review process. The accrediting official has determined that compliance reviews adequately test the security implementation for each.

5.5 Modification Controls

The U/SO is responsible for bringing all planned system modifications to the attention of the ISSO at the earliest opportunity. All modifications planned for accredited IS equipment will be discussed with the ISSO prior to implementation. The ISSO will analyze the proposed modification to determine the expected impact on security caused by the changes and, if applicable, gain any approval required of the TEMPEST Coordinator, SO-332/GTN, or other security official. In addition, the Individual Security Plan must be updated to reflect the modification, and forwarded with appropriate Attachments for certification and reaccreditation (See also, Paragraph 17 for applicability.)

5.6 Periods Processing

5.6.1 Fax Devices

Fax devices are accredited for use in the Digital Interface (DI) mode only to process classified information. They may not be used in the Public Switched Data Network (PSDN) mode to process unclassified information. Therefore, periods processing is limited to varying levels of classified information only. All documents sent or received using an accredited Fax device must be appropriately marked, handled and protected as classified if necessary until reviewed by an authorized classifier.

5.6.2 Digital Copiers

Unlike accredited fax devices, digital copiers may be used to duplicate classified as well as unclassified documents using periods processing. Periods processing is the term used to describe the method of operation where information of one specific level of classification is processed, the copier is sanitized to eliminate any residual classified information, and then either a lower

level of classified information or unclassified information is processed. This cycle is repeated each time information of differing levels of classification is sequentially processed.

5.7 Maintenance Swap Controls

5.7.1 Fax Devices

If hardware failure requires replacement of an accredited Fax device, before the replacement is used for classified information the device must be security tested using the Security Review Checklist for Fax Device Certification Attachment 4F. Additionally, the ISSO must ensure that all prohibited features have been disabled on Fax devices. See Paragraph 12.4.3 for the list of prohibited features. The verification log report may be used for this purpose.

5.7.2 Digital Copiers

Digital copiers come with various internal memory configurations up to 32 megabytes. Some even come with internal disk drives used as temporary storage when processing large or graphics intensive jobs. For this reason, if the copier cannot be replaced by the exact model, including features, it must undergo recertification/reaccreditation before being used to process classified information.

Digital Copiers with internal hard disks must be marked internally (on the disk housing) and externally with the highest classification and most restrictive category of information for which the copier has been approved to reproduce. Further, if the disk drive is removable it must be stored in a security container (during non-duty hours). If the disk drive is not removable the copier must be located in a security area approved for open storage at the same level/category as the disk. Copiers with Internal classified hard disk drives must also be noted on the respective individual security plan, Attachment 5F.

5.8 Acquisition Specification

DOE and DOE Contractor organizations shall ensure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition of hardware, software, or related services to be utilized in a classified environment. The ISSM will be included in the planning process for any new hardware or software procurement or developments that apply to classified in the DOE HQ environment.

(THIS PAGE INTENTIONALLY LEFT BLANK)

6. PERSONNEL SECURITY

Appropriate measures will be taken by the Fax device/digital copier operators to ensure that personnel without appropriate access authorization do not have physical or visual access to the classified documents being processed. Access to STU-III/Fax devices and digital copier equipment will be restricted to trained, authorized users, who are thoroughly familiar with the procedures for processing classified Faxes and duplication of classified documents.

6.1 Fax Device Operators

Each accredited Fax device will have at least one (1) primary and one (1) alternate operator assigned responsibility for the operation and security of the device and the classified information processed by the device. All operators will be cleared for the highest level and most restrictive category of information for which the Fax device has been approved to process.

6.2 Digital Copier Key Operators

Each accredited digital copier will have at least one person assigned responsibility as the key operator. The key operator is the person primarily responsible for the security of the equipment, training of other staff members in the operation and security of the equipment and information reproduced on the equipment.

6.3 Clearance Verification

Accredited Fax device operators will visually verify that the clearance level of personnel requesting transmission or receipt of a classified Fax is appropriate to the level of classification of the documents processed.

(THIS PAGE INTENTIONALLY LEFT BLANK)

7. PHYSICAL SECURITY

General physical security requirements and building access controls can be found in the DOE HQ Facilities Master Security Plan, Chapter IV, Physical Protection Program.

7.1 Security Areas for Accredited Fax Devices/digital Copiers

Accredited Fax devices/digital copiers within the HQ complex (Germantown and Forrestal buildings) must be physically located within:

- **!** A vault or vault-type room authorized for the open storage and the processing of classified information; or,

- **!** A limited area. A security area which is established for protection of classified matter where security officers or other internal controls can prevent access to classified matter by unauthorized persons; or

- **!** An exclusion area. A security area which is established for protection of classified matter where mere presence in the area would normally result in access to classified information.

7.2 Mode of Operation - Fax Devices

Accredited fax devices may be operated in the stand-alone automatic answer, with the Crypto Ignition Key (CIK) activated provided the STU-III is constantly attended (see **exception** below). When the STU-III is left unattended for any length of time, The CIK must be removed and properly stored. During classified transmission or reception, an appropriately cleared person must have visual contact with the fax device.

(EXCEPTION) A fax device may operate in the stand-alone , unattended mode with the CIK activated only when it is located in a vault which has been approved for open storage of classified information. Provided the level of the STU-III CIK does not exceed the level of the open storage authorization.

7.3 Placement and Control

Once installed, accredited fax devices and digital copiers may not be moved from the room in which it was installed without the express permission of the

responsible ISSO. They must remain in the room where they were installed until their movement or reinstallation elsewhere is approved by the ISSO. The ISSM will provide an “Approved for Classified” label that must be affixed to the cabinet, where it can be easily seen. See Paragraph 5.7.2 for marking requirements for digital copiers with internal fixed disk drives.

(Note: The “Approved for Classified” stickers must be removed if the equipment is relocated outside of a security area, returned to storage, sent out for repair, etc.) Digital copiers with fixed internal disk drives must have them removed before the copier can be moved out of the security area where they are installed.

8. TELECOMMUNICATIONS SECURITY

Each communications link used to support accredited Fax devices is protected commensurate with the level of classification and category of the information for which the system is accredited. The protection features of each link are implemented in accordance with DOE M 200.1-1, Telecommunications Security Manual.

8.1 Digital Copiers

Digital copiers accredited to process classified information may not be connected to any telecommunication line for any reason.

8.2 Stu-III Secure Voice/data Set (SV/DS)

The only dial-up, point-to-point communications authorized for use with classified information among accredited Fax devices are those provided by National Security Agency-approved encryption devices (e.g., STU-III SV/DS). Reference Paragraph 10.o (3) page XI-35 - XI-36, DOE Headquarters Facilities Master Security Plan.

Section III of the Individual Facsimile Device/Digital Copier Security Plan (Attachment 5F) will be appropriately annotated and the system accredited by the ISSM prior to use. An "Approved for Classified" label must be affixed to the STU-III SV/DS prior to any classified data transmission.

The person sending a classified Fax is responsible for verifying that the recipient and the facility where the fax is to be sent is authorized to receive and properly store the transmitted classified information. This is accomplished through the Safeguards and Security Information Management System (SSIMS) and the classification level shown on the STU-III display when the device is placed in the secure mode.

- Before a secure data transmission can begin, contact must be made with the receiving station. Verification of the distant party's identification and telephone number must be made during the contact.

- To initiate secure Fax transmission, a valid Cryptographic Ignition Key must be inserted into the STU-III SV/DS and confirmation of the secure mode must be received and indicated.

- **!** Only properly cleared personnel with the proper "need-to-know" should access Fax devices during the entire period of interconnection. This ensures by visual verification that the proper classification level and identification information of the STU-III SV/DS display matches the classification of the data being transmitted and the recipient's need-to-know.

- **!** It is the responsibility of both sender and receiver to ensure that no data is transmitted that is of a higher classification level or more restrictive category than their highest common clearance/access level, the classification level of the STU-III CIK, and the classification level for which the Fax device has been accredited.

- **!** To prevent a higher classification of data being sent than is authorized, visual inspection of the data before transmission by the sender is mandatory.

- **!** The automatic logging feature will be used, if available, to document all Fax traffic.

8.3 Accredited Fax Devices

Accredited Fax devices have two different communications modes (1) Digital Interface (DI) and (2) Public Switched Telephone Network (PSTN). Accredited Fax devices are set up to emulate the DI communications mode through a RS-232 connection to a STU-III device for secure communications of classified information. Fax devices at HQ are accredited to process **in DI mode (encrypted) only.** The PSTN options/functions must be disabled.

8.3.1 Procedures for Classified Fax Authentication - Send

The responsibility for verifying that the recipient is authorized to receive classified material rests with the sender. The operator of the sending accredited Fax device must be satisfied that verification has been accomplished prior to transmission. Prior coordination with the recipient is required. Individuals transmitting classified information electronically must confirm receipt (either written or verbal) with the intended recipient.

8.3.2 Procedures for Classified Fax Authentication - Receive

The intended recipient (the person to whom the Fax is addressed) of an incoming classified Fax should contact the operator of the accredited Fax device

that will be receiving the Fax and give notification of an expected classified Fax. Upon contact with the sender and or recipient of an incoming classified Fax, the operator of the receiving accredited Fax device must: (1) verify the classification level and category of the Fax, normally not to exceed secret, (2) verify that the number of pages received is the same as what is stated on Fax cover sheet, (3) sign and send a copy of the receipt for classified matter to the sender either via Fax or mail, (4) protect the classified document accordingly, (5) notify the recipient of receipt and (6) notify the sender of any discrepancies noted during transmission.

Note: Fax operators transmitting classified documents shall confirm receipt (written or verbal) with the intended recipient. If verbal confirmation is received, the sender will annotate on the first page of the transmittal the name of the individual who received the transmission and the number of pages, the time and date the transmission was received.

8.4 Emission Security

The ISSO ensures a pre-installation site survey is performed to ensure that the site is suitable for accredited system placement. Aperiodic checks are also performed by the ISSO and the ISSM to ensure continued compliance.

DOE Red/Black separation requires a minimum of: Six (6) inches of separation between classified IS (the entire system, including peripheral devices) and any part of an unclassified IS (entire system, including peripheral devices); A minimum of two (2) inches of separation between classified and unclassified data lines.

There must be six (6) inches of separation between classified IS and telephones; and six (6) inches of separation between STU-III devices and classified and unclassified IS.

In addition to the separation requirements above, all classified data lines must be marked with red tape at the point of connection to the classified IS and at intervals that allow for easy recognition of those lines. Reference DOE M 200.1-1, Telecommunications Security Manual, Chapter 7, Emissions Control (Part 1), dated 3/15/97, for specific details of separation requirements.

The separation requirements specified above do not apply to IS currently operating in an area that is covered under a TEMPEST Plan. Separation requirements for these systems are specified in their applicable TEMPEST Plan, and maintained by the Headquarters TEMPEST Coordinator, SO-332/GTN. |

Consultation with the TEMPEST Coordinator should be effected for those systems planned for these areas.

8.5 Remote Diagnostic Services

Remote diagnostic services are prohibited on accredited Fax devices and Digital Copiers.

9. SOFTWARE SECURITY

9.1 Digital Copiers

Some digital copiers utilize stored software to perform some of it's functions. This software is usually installed in read only memory. Software maintenance usually must be performed by the equipment manufacturer. Consult with the ISSM before loading/installing software.

9.2 Fax Devices

Not applicable to Fax devices.

(THIS PAGE INTENTIONALLY LEFT BLANK)

10. ADMINISTRATIVE SECURITY

10.1 Access Controls

The crypto ignition key for the STU-III limits use of the accredited Fax device to authorized operators/users. If an accredited Fax device is equipped with an access code feature (similar to a password on a computer), the feature may be used to provide additional access control.

10.2 Printed Output

All documents received by a Fax device during classified sessions should have been properly marked by the sending organization prior to being transmitted. However, if unmarked documents are received they will be handled, stored, and protected as if they contained the highest classification level and most restrictive category of data for which the Fax device is accredited to process until properly reviewed by an authorized derivative classifier. All printed output of digital copiers must be reviewed to ensure that classification markings are consistent with the original documents they were copied from. It will be necessary to mark the last page with the overall classification level.

If material received requires accountability, appropriate actions will be taken by the control point operator/document custodian prior to distribution of the material.

10.3 Toner Cartridges

Sanitized toner cartridges may be left in fax devices and digital copiers without being marked with a classification label as long as the fax device or copier is in proper working order and has not malfunctioned during operation, i.e. paper jam, etc., see Paragraph 10.6.3. for information on machine malfunctions. See Paragraph 10.6.4 for information on depleted toner cartridges.

10.4 Thermal Transfer Rolls

Some Fax devices use a thermal transfer roll in place of a ribbon or toner cartridge. Once used, the information that has been printed can be read on the roll. For this reason the roll must be marked with classification labels appropriate to the highest level and most restrictive category of information for which the Fax device or digital copier has been accredited to process, removed from the device and stored in an appropriate security container when the device

is unattended. When the classified roll is depleted and replaced, the old one must be destroyed appropriately (see Paragraph 10.5 below).

10.5 Destruction Procedures

Destruction of classified documents (including classified printer ribbons, thermal transfer rolls, etc.) is accomplished in accordance with instructions found in chapter XI Classified Matter Protection and Control of the DOE Headquarters Facilities Master Security Plan.

10.6 System Sanitization

10.6.1 Fax Devices

Before being left unattended accredited Fax devices must be sanitized using the following procedure:

- Remove all classified documents from the device paper trays;
- Make sure that the device has not run out of paper or malfunctioned while receiving a classified document. Make sure that the number of pages received is the same as the number specified on the cover page and the device's page counter;
- Remove the CIK from the STU-III and store it in an approved storage container;
- Open the device and inspect to ensure that no classified documents remain inside;
- Turn off the electrical power to the device for at least two (2) minutes to erase the memory. Turn on the electrical power to the device.

10.6.2 Digital Copiers

After reproduction of classified information digital copiers must be sanitized using the following procedure:

- Turn off the power to the copier for two (2) minutes.
- Check the reproduction path and all paper trays inside the copier to ensure there are no classified documents present. Be especially careful

when double sided copying has been performed. Any remaining classified matter must be handled and disposed of in a manner approved for classified destruction. Turn power on.

10.6.3 Toner Cartridges

Laser printer toner cartridges no longer need to be cleared or sanitized by printing 3 pages of random characters as long as the last print process was successfully completed. In the case of a paper jam, power failure during printing, etc., reprinting the document successfully will satisfy the need to clear or sanitize the toner cartridge.

Once sanitized, the laser printer toner cartridge may be released to unclassified channels for replenishment.

10.6.4 Depleted Toner Cartridges

Some Fax devices will not function when their toner cartridge has been totally depleted, therefore the toner cartridge cannot be sanitized for recycling and must be destroyed as classified waste.

(THIS PAGE INTENTIONALLY LEFT BLANK)

11. WASTE, FRAUD, AND ABUSE

11.1 Definition and Reporting

Waste, fraud, and abuse incidents in which computers and/or their peripherals are involved are to be reported and addressed through the perpetrator's direct line of management. These types of incidents are a violation of the Code of Federal Regulations and the Federal Employees Code of Ethics.

The definitions of waste, fraud and abuse are as follows:

Waste - Misuse of computer time (i.e., games, private use, use of unauthorized software), or resources, whether intentional or not.

Fraud - Illegal activities, including misrepresentation, personal gain, copyright violations.

Abuse - Intentional alteration or destruction of software, hardware, or information.

(THIS PAGE INTENTIONALLY LEFT BLANK)

12. RISK IDENTIFICATION

A qualitative risk identification has been performed for accredited fax devices at the Germantown and Forrestal facilities. This identification is general in nature because it encompasses all fax devices within these facilities. The level of protection provided each fax device is based on the U/SOs knowledge of the security procedures detailed in this plan.

Digital copiers are unique and will require a detailed risk identification by technically knowledgeable personnel.

12.1 Risk Identification

The following table (continued on next page) identifies some specific risks to accredited fax devices and digital copiers, their probability of occurrence rating (i.e., Low, Moderate, High), the impact of an occurrence, and implemented countermeasures.

RISKS	PROBLEM	IMPACT	COUNTERMEASURE
Fire	Low	High	Fire extinguishers, some areas protected by fire suppression systems.
Power Disturbances	Low	Low	Fax devices protected by surge protection devices. Other copying machines are available.
Power Outages	High	Low	Other methods are available to transmit and copy classified information.
Water Damage	Low	Low	Construction of building and placement of Fax devices and digital copiers negates water damage.
Malicious Authorized U/SOs	Low	Low	All U/SOs processing classified have security clearances and have been trained in the protection of classified information and the systems that process classified information.
Covert Action	Low	Low	Building guards, visitor controls, and use of approved safes for document storage. Limited Security Areas with electronic and combination locks control access. Hardware procurement, installation, and support cannot be targeted to accredited Fax devices and digital copiers.

RISKS	PROBLEM	IMPACT	COUNTERMEASURE
Casual Visitors	Low	Low	Posted signs for classified processing, room divider around accredited Fax devices in some rooms, visitor controls, 3-way combination locks and limited security areas control access.
Emanation	Low	Low	Use of TEMPEST-protected or other DOE-approved low-emanation equipment.
Natural Hazards	Low	Low	Inherently secure/safe buildings.
System Abuse	Moderate	Low	Monitoring by supervisor and the ISSO. Personnel security briefings. Regular Waste, Fraud, and Abuse surveys.
Certain Features on Fax Devices and Digital Copiers	Low	Moderate	Fax device features that pose a vulnerability are disabled. Digital copier features that pose a vulnerability such as Fax module are not installed. Periodic physical checks ensure prohibited features remain disabled.
Untrained Personnel	High	High	Untrained personnel pose a serious concern. Properly trained employees insure that security measures outlined herein are addressed.

12.2 Asset Identification

All items of IS equipment are considered low value assets. Each equipment asset will be identified in the Individual Security Plan.

12.3 Summary of Qualitative Risk Identification

The qualitative risk identification chart, Paragraph 12.1, depicts the risk management technique used to identify and counter all known and potential risks. Based on the analyses of these risks and the fact that all classified processing is performed within DOE Security Areas, the protection mechanisms implemented for these areas are deemed sufficient for the low value assets covered by this plan. Except for IS equipment located in vaults approved for open storage of classified information, see Chapter II of DOE M 471.2-1 Manual for Classified Matter Protection and Control for specific guidance on the control of all classified media. All classified media must be controlled (if necessary) by document-accountability procedures. The protection mechanisms implemented within the Security Areas for the protection of documents have been evaluated

by the ISSM and deemed sufficient for the protection of the information processed.

12.4 Accredited Fax Device Risk Vulnerability, Countermeasures, and Prohibited Features

12.4.1 Countermeasures

Accredited Fax device features that pose security vulnerabilities must be disabled. A Transaction Confirmation Report will be printed monthly and checked to ensure the features of the accredited Fax device remain in the disabled positions. Additionally, the machine will be physically checked, prior to the transmission of classified matter, to ensure the PSTN transmission mode (see discussion of communications modes in Section 5.6, Periods Processing) has not been physically established.

12.4.2 Allowed (Enabled) Features/functions (Note: Feature names may vary between Fax Devices/Manufacturers. This list common the Ricoh SFX2800M)

The features/functions in the following list must be enabled:

(1) Clock Adjustment:	Enabled
(2) Communicated Page Counter:	Enabled
(3) Department Code On/Off:	Enabled
(4) Digital Interface Parameter List:	Enabled
(5) Edit or Create Digital Interface Mode:	Enabled
(6) Load or Delete Digital Interface Mode:	Enabled
(7) Page Count On/Off:	Enabled
(8) Printing a Transaction Confirmation Rpt:	Enabled
(9) Printing the Number List:	Enabled
(10) Programming the ID Code:	Enabled
(11) Programming End Messages:	Enabled
(12) Programming Remote Terminal ID:	Enabled
(13) Programming Transmit Terminal ID:	Enabled
(14) Programming DI Mode Password:	Enabled
(15) Scanned and Printed Page Counter:	Enabled
(16) Select Date & Time on Reports Control:	Enabled
(17) Switching Super Smoothing On/Off:	Enabled
(18) Switching Transmit Terminal ID On/Off:	Enabled
(19) Transmission Report On/Off:	Enabled

12.4.3 Prohibited (Disabled) Features/Functions

The features/functions in the following list must be disabled:

(1)	Authorized Reception On/Off:	Disabled
(2)	Clearing Memory Files:	Disabled
(3)	Clearing Polling Files:	Disabled
(4)	Forwarding On/Off:	Disabled
(5)	Printing a Confidential Message:	Disabled
(6)	Printing the Authorized Reception List:	Disabled
(7)	Printing the Contents of a Memory File:	Disabled
(8)	Printing the Polling File List:	Disabled
(9)	Printing the Program List	Disabled
(10)	Printing the Store and Forward File List:	Disabled
(11)	Programming Authorized Reception:	Disabled
(12)	Programming the Confidential Password:	Disabled
(13)	Programming Called Subscriber ID:	Disabled
(14)	Programming Groups:	Disabled
(15)	Programming a Forwarding Telephone #:	Disabled
(16)	Program Fax Terminal's Telephone #:	Disabled
(17)	Reception Mode Switching Timer:	Disabled
(18)	Send Later:	Disabled
(19)	Switching Error Correction Mode On/Off:	Disabled
(20)	Telephone Line Type Selection:	Disabled
(21)	Volume Adjustment:	Disabled
(22)	Multi-copy:	Disabled
(23)	Polling Transmission/Reception:	Disabled
(24)	Printing the Quick Dial Character List:	Disabled
(25)	Programming Quick Dial Characters:	Disabled
(26)	Programming Quick Dial and Speed Dial:	Disabled
(27)	PSTN Mode Enable/Disable:	Disabled
(28)	Switching PSTN Busy On/Off:	Disabled

13. TRAINING

13.1 ISSOS

All ISSOs are required to attend the ISSO Training Class provided by the ISSM. As a minimum, the ISSOs will provide the following instructional material to each U/SO.

- **Master IS Security Plan for Facsimile Devices and Digital Copiers**. The ISSO and U/SO must retain a copy of the currently approved Master IS Security Plan for Facsimile Devices and Digital Copiers at their respective systems. These copies may be maintained in an electronic format (as a data file), in lieu of maintaining a printed copy. Electronic copies of the Plan and its Attachments (blank forms) may be obtained by downloading from the DOE Headquarters Computer Security Web Site at: http://cio.doe.gov/compsec/

13.2 U/SOS

Each responsible U/SO (Fax device operators, and digital copier key operators) will read the Master IS Security Plan for Facsimile Devices and Digital Copiers. The responsible U/SO will, also annually, sign Attachment 1F, User/Security Officer Code of Conduct, accepting responsibility for the security of their assigned IS equipment.

13.3 Computer Security-Trained Escorts.

To qualify as a computer security-trained escort, the candidate must have received all the training listed in the previous Paragraph for U/SOs and must be technically competent to escort and observe repair technicians. Questions concerning technical competence will be determined by the ISSO.

(THIS PAGE INTENTIONALLY LEFT BLANK)

14. INCIDENT REPORTING

In order to thwart deliberate and/or malicious acts (i.e., equipment tampering, etc.,) directed at IS equipment, all personnel utilizing DOE IS equipment resources will observe the following procedures for reporting any perceived attacks. Also, any occurrence of a security infraction will be reported using the procedures below. These procedures will permit each U/SO to properly report potentially damaging incidents. By initiating the following actions in a timely manner, U/SOs may assist in controlling and limiting the damage that may be caused by an incident.

14.1 Incident Recognition by U/SO

Upon noticing or suspecting unusual or uncharacteristic performance from your system, suspend processing on the affected system. Attempts to determine the cause through use of the system may distort or destroy any evidence investigators might need to identify and/or correct the situation.

14.2 Notification Procedures

U/SOs are to immediately notify, through secure means (e.g., face-to-face, encrypted voice), the responsible ISSO (and/or Alternate ISSO) of the affected system concerning the possibility of a successful threat occurrence. This will allow the ISSO to immediately begin a preliminary inquiry and notify other potential targets, thereby limiting further potential damage. If the ISSO or Alternate is not readily available, call the ISSM. Minor incidents associated with the use of IS equipment (generally those whose adverse impact can be contained within the authority and responsibility of the ISSO) need not be reported to the ISSM, but are to be documented, investigated, and resolved by the ISSO.

Incidents whose scope and adverse impact extend beyond the authority and responsibility of the ISSO are to be communicated to the ISSM as soon as practical. The intent is to coordinate efforts to limit the potential damage which could be incurred.

14.3 Documentation and Review

After incident notification, the U/SO will annotate the following information, if known, for use by security personnel.

a. Time of Occurrence

b. Source of Problem

c. Nature of the Incident - explain what happened prior to and during the occurrence.

d. The U/SO should review DOE Headquarters Facilities Master Security Plan Chapter XVI, Security Incidents/Infractions/Violations Program for more guidance.

e. Personnel involved, witnesses, etc.

f. Classification level and category of information.

15. CONTINGENCY PLANNING

In general, IS equipment assets are low cost, easily replaceable items. However, contingency planning is addressed for all systems that process classified information, as follows.

It is the responsibility of the U/SO to identify any hardware configuration or software system that is considered critical for the successful completion of the DOE mission. If a system is designated as critical, backup procedures and matching system configurations must be identified in writing to ensure continuity of operations. Additional procedures, specific to the critical system, will be identified in the Individual Security Plan for the critical system. These procedures must be tested annually.

16. ESCORT PROCEDURES

Visitors (cleared, but without a need-to-know, or uncleared) to office areas where accredited Fax devices and/or digital copiers are present must be escorted in accordance with DOE Headquarters Facilities Master Security Plan and may not be permitted physical access to accredited Fax devices and/or digital copiers or to view classified information. In addition, escorts for visitors who are going to have access to the inside of an accredited Fax device and/or digital copier (uncleared repair technician) must be computer security-trained in accordance with Paragraph 13.3 of this plan.

17. INTERIM OPERATING PROCEDURES

The following procedures govern the operations of an accredited Fax device in the interim periods during updates or changes to their environment. The environment of an accredited Fax device encompasses the hardware listed in Attachment 5; the location of the IS equipment; the assigned U/SO; and, the approved security controls in place at the time of the current accreditation.

Interim reaccreditation is granted for a period of 10 work days only for those systems previously accredited and only under the following conditions: |

- U/SO Changes,
- Hardware replacement with similar equipment, or
- System relocations within an existing like security area only.

Interim accreditation begins when the change is effected (e.g., hardware has been reinstalled at the new location) and the device has been security tested and recertified by the ISSO.

If not reaccredited in these 10 work days, the system will be considered unaccredited and will only be authorized to process unclassified information after being sanitized.

18. AUDITING

Auditing for accredited Fax devices will be accomplished by the ISSO through the monthly Transaction Confirmation Report, and Automated Facsimile Activity Log.

FACSIMILE DEVICE/DIGITAL COPIER USER/SECURITY OFFICER CODE OF CONDUCT

Initials of U/SO		
1. _____	I have read the Master IS Security Plan for Facsimile Devices and Digital Copiers and the pertinent sections of the DOE Headquarters Facilities Master Security Plan concerning classified facsimile devices and/or Digital Copiers.
2. _____	I am aware of my responsibility for knowing what constitutes a security infraction and the procedures for responding to an infraction.
3. _____	I am aware of my responsibility for reporting any security-related events involving the Facsimile device to the Classified IS Security Officer (ISSO) in accordance with current DOE and local policy.
4. _____	I am aware that, when the Facsimile device or Digital Copier is not in use and/or is to be left unattended, it must be sanitized by turning off the electric power for at least 2 minutes, turning the power on, and off a second time for at least 2 minutes. classified documents that have been processed must be locked in a DOE approved security container, the Crypto Ignition Key (CIK) for the STU-III used with facsimile devices must be removed from the STU-III and placed in a security container.
5. _____	I am aware that users of classified Fax devices and/or Digital Copiers are to prevent (to the extent possible) unauthorized persons from entering the work area during classified processing and that the Facsimile device/Digital Copier must be positioned so that it cannot be viewed from outside the processing area (i.e., in view from open doors or uncovered windows).
6. _____	I am aware that classified documents (sent or received by the Facsimile device) and/or reproduced by a digital copier and their covers or containers must bear appropriate classification markings that indicate the highest level of data contained therein. I am further aware of my responsibility to follow Document (or Media) Accountability Procedures located in Chapter XI Paragraph 5 of the DOE Headquarters Facilities Master Security Plan.
7. _____	I am aware that toner cartridges used for classified processing need to be sanitized only when the FAX device or digital copier has malfunctioned. I am aware that the DOE HQ Master IS Security Plan for Facsimile Devices and Digital Copiers Paragraphs 10.6.3 and 10.6.4 provide guidance foe sanitizing toner cartridges.
8. _____	I am aware of my responsibility to continually improve security. Through my daily interaction with a facsimile device and/or digital copier, I am able to detect weaknesses and vulnerabilities within the system. I will make a conscientious effort to express ideas on enhancing security to the designated Classified IS Security Officer.
9. _____	I am aware that, as a U/SO of Department of Energy office systems, I must ensure that the equipment is used only for job related processing and that all other uses are prohibited. I am aware that I am subject to periodic review for compliance and audit for waste, fraud, and abuse by my management and other internal and external auditing agencies (i.e., IG, GAO, etc.).

10. _____ I am aware that electronic equipment, antennas, etc., may not be placed in the immediate proximity of the classified facsimile device and/or digital copier without being listed and approved by the ISSM in the Individual Facsimile Device/digital copier Security Plan. I am also aware that any modifications to the device may not be performed without the prior approval of the ISSO.

Statements 11 & 12 are for Users of Facsimile Device only

11. _____ I am aware that I am responsible for ensuring that the sender verifies that the receiver has the proper clearance and need-to-know for outgoing classified documents.

12. _____ I am aware that it is my responsibility based on notification by the sender or addressee to verify the classification level and category of incoming documents, not to exceed Secret, send requested document receipt to the sender,

I have read the above statements and understand my responsibilities for protecting classified office systems and information as indicated by my initials. I am aware that I am required to review, initial, and resign this attachment annually no later than the anniversary date as indicated next to my signature below.

U/SO: _____ _____ ___/___/___
Printed Name *Signature* *Date*

****

Facsimile Device/Digital Copier User/Security Officer
Code of Conduct - Instructions

The purpose of this attachment is to provide a documented means of insuring that each U/SO is aware of his/her responsibilities for processing classified information on an accredited facsimile device/Digital Copier.

This attachment contains a series of statements, for which the U/SO will initial each to indicate that he/she understands and acknowledges his/her responsibilities. This will be done annually (not later than 1 year from the date signed on the previous attachment) by each U/SO to provide a refresher to the U/SO of his/her responsibilities. After the U/SO has completed this attachment (all the statements are initialed) and the ISSO is confident that the U/SO understands his/her responsibilities, then the ISSO may allow the U/SO to perform classified processing on an accredited facsimile device and/or Digital Copier. This attachment is not required to be submitted with the accreditation/reaccreditation package to the ISSM, but will be reviewed by the ISSM representative when a site or compliance review is held. The ISSO will retain the original of this attachment until replaced by the next annual attachment completion and provide a copy of same to the U/SO for reference purposes.

HQ ACCREDITATION /REACCREDITATION PERIOD MATRIX

The below listed matrix outlines the maximum information systems security (ISS) accreditation periods for HQ ISS. This matrix reflects the risk and subsequent review of ISS system protection strategies:

Risk Level	Time	Conditions
Low	36 months	No ISS deviations or HQ Attachment 8's (Statement of Security Risk).
		Information System located in an approved security area.
		Information System using Windows Win NT 4.0 (+) with enabled security features, i.e., passwords, user accounts, audit procedures, account restrictions, etc.
		Level of concern for Information System confidentiality, integrity or availability is medium or low.
		Protection Level of 1 or 2.
Medium	18 months	All classified Information System Networks.
		Any Information System using a STU-III/data encryption device.
		An Information System with an ISS deviation or an Attachment 8.
		All digital copiers or classified facsimile devices.
		Personal Computers/Information Systems NOT using Win NT 4.0 (+) (without a security deviation or Attachment 8).
		Protection Level of 1 or 2.
High	12 months	Whenever a level of concern for Information System confidentiality, integrity or availability is high.
		Protection Level of 3.
Excessively High	6 months	HQ DOE Laptops/PDAs (limited to Secret).
		Personal Computers/Information Systems NOT using Win NT 4.0 that have an ISS deviation or an Attachment 8.
		Any Information System (digital copiers, classified Fax or ISS) approved to process classified outside of formally established HQ limited/exclusion security areas.

Excessively High	**6 months**	**Non HQ DOE Information System (Forrestal/Germantown only).** **Any Information System using internal/external microphones, video cameras or infrared transmit/receive port(s).** **Protection Level of 4 or higher.**

(Note: Attachment 8 is part of the HQ Master IS Plan to reflect increased risk.)

Provisional accreditations will be granted to operate an IS because of incomplete documentation or to permit a major conversion of a system. However, the necessary security countermeasures must be in place and functioning during this interim accreditation. Further, these provisional accreditations will not exceed 90 days.

SECURITY REVIEW CHECKLIST
FOR FACSIMILE DEVICE/DIGITAL COPIER CERTIFICATION

SYSTEM ID: HQ-_____(ISSM will Assign) **DATE: _____/_____/_____** **ORGANIZATION: _____**

LOCATION: BUILDING _____ **ROOM NUMBER _____**

	PRINTED NAME	SIGNATURE	DATE
Operator			
ISSO			
HSO			
REVIEWED BY			
ISSM STAFF MEMBER			

COMPLETE THIS SECTION FOR FACSIMILE DEVICES & DIGITAL COPIERS	YES	NO
1. IS THE CERTIFICATION DOCUMENTATION COMPLETE AND ACCURATE?		
2. IS THE EQUIPMENT LOCATED IN A LIMITED SECURITY AREA, EXCLUSION AREA OR A VAULT/VAULT TYPE ROOM?		
3. IF THE EQUIPMENT IS LOCATED IN AN APPROVED VAULT, IS THERE EVIDENCE OF CERTIFICATION FROM THE HEADQUARTERS OPERATIONS DIVISION (SO-213) DOCUMENTING THEIR APPROVAL FOR OPEN STORAGE OF CLASSIFIED DATA?		
4. ARE LIMITED SECURITY AREA WARNING SIGNS AVAILABLE FOR THE DOORS LEADING TO THE ROOMS WHERE THE EQUIPMENT IS LOCATED?		
5. IS THE U/SO AWARE OF THE CLASSIFIED DOCUMENT/MEDIA MARKING/LABELING PROCEDURES AND IS THERE EVIDENCE OF ADEQUATE SUPPLIES OF LABELING STOCK? IF THIS IS A REACCREDITATION REVIEW, IS THERE EVIDENCE OF PREVIOUS COMPLIANCE WITH MARKING/LABELING PROCEDURES?		
6. IS THE U/SO AWARE OF THE PROPER PROCEDURES FOR COMPLYING WITH CLASSIFIED DOCUMENT/MEDIA ACCOUNTABILITY REQUIREMENTS? IF THIS IS A REACCREDITATION REVIEW, IS THERE EVIDENCE OF PREVIOUS COMPLIANCE WITH ACCOUNTABILITY REQUIREMENTS?		
7. IS THE EQUIPMENT MAINTAINED AND SUPPORTED BY THE CIO (OR, IF EQUIPMENT IS NOT MAINTAINED AND SUPPORTED BY THE CIO, HAVE MAINTENANCE PROCEDURES BEEN APPROVED BY THE ISSM AND INCLUDED IN THE INDIVIDUAL FAX DEVICE/DIGITAL COPIER SECURITY PLAN)?		
8. RED/BLACK SEPARATION IN COMPLIANCE?		
9. IS THE U/SO AWARE THAT THEY ARE RESPONSIBLE FOR BEING PRESENT DURING THE ENTIRE TIME A CLASSIFIED DOCUMENT IS BEING COPIED, SENT OR RECEIVED?		
COMPLETE THIS SECTION FOR FACSIMILE DEVICES	**YES**	**NO**
10. ARE WRITTEN PROCEDURES FOR AUTHENTICATION IN THE RECEIVE AND SEND MODE POSTED NEAR THE SYSTEM, AND ARE THEY FOLLOWED?		
11. IF APPLICABLE, AND IF THIS IS AN INITIAL CERTIFICATION REVIEW, IS THE U/SO AWARE OF PROCEDURES FOR USING A STU-III SV/DS OR SDD FOR DATA COMMUNICATIONS? IF APPLICABLE, AND IF THIS IS A REACCREDITATION REVIEW, IS THERE EVIDENCE OF COMPLIANCE WITH THE PROCEDURES?		

FACSIMILE DEVICES (CONTINUED)	YES	NO
12. IS THE U/SO AWARE OF THE REQUIREMENT TO VERIFY THAT THE FAX DEVICE IS IN THE DI MODE, THAT ALL PROHIBITED FEATURES ARE DISABLED AND THAT ONLY THE STU-III IS CONNECTED TO THE UNIT PRIOR TO SENDING OR RECEIVING CLASSIFIED DOCUMENTS?		
13. HAS U/SO READ THE DOE HEADQUARTERS MASTER IS SECURITY PLAN FOR FACSIMILE DEVICES & DIGITAL COPIERS AND THE STU-III PROCEDURAL GUIDE?		
14. ARE WRITTEN PROCEDURES IN PLACE TO ENSURE THAT THE FAX DEVICE HAS PROCESSED ALL PAGES OF INCOMING DOCUMENTS AND HAS NOT RUN OUT OF PAPER, THAT THE CIK HAS BEEN REMOVED, THE POWER IS TURNED OFF AND ALL DOCUMENTS ARE REMOVED FROM THE UNIT BEFORE BEING LEFT UNATTENDED AND AT THE END OF THE DAY?		
COMPLETE THIS SECTION FOR DIGITAL COPIERS	**YES**	**NO**
15. ARE WRITTEN PROCEDURES IN PLACE TO ENSURE THAT THE DIGITAL COPIER HAS PROCESSED ALL PAGES OF THE DOCUMENTS BEING COPIED AND HAS NOT RUN OUT OF PAPER, THAT NO INPUT OR OUTPUT DOCUMENTS HAVE BEEN LEFT IN THE PAPER PATH, THE POWER IS TURNED OFF AND ALL DOCUMENTS ARE REMOVED FROM THE UNIT WHEN A CLASSIFIED COPY JOB IS COMPLETE, BEFORE BEING LEFT UNATTENDED AND AT THE END OF THE DAY?		
16. HAS U/SO READ THE DOE HEADQUARTERS MASTER IS SECURITY PLAN FOR FACSIMILE DEVICES & DIGITAL COPIERS?		
17. IF THE DIGITAL COPIER IS EQUIPPED WITH A FIXED DISK DRIVE DOES THE COPIER HAVE STICKER AFFIXED THAT INDICATES THE HIGHEST LEVEL AND MOST RESTRICTIVE CATEGORY OF CLASSIFIED INFORMATION FOR WHICH THE COPIER HAS BEEN (OR WILL BE) APPROVED TO PROCESS?		
18. IF THE COPIER IS EQUIPPED WITH A DISK DRIVE AND IS NOT LOCATED IN A VAULT APPROVED FOR OPEN STORAGE, IS THE DISK DRIVE STORED IN AN APPROVED SECURITY CONTAINER DURING NON-DUTY HOURS?		
19. ARE PROCEDURES FOR SANITIZING DIGITAL COPIERS POSTED WHERE THEY CAN BE EASILY SEEN?		
20. DO SANITIZATION PROCEDURES INCLUDE: CHECKING PAPER TRAYS AND PAPER PATHS FOR CLASSIFIED DOCUMENTS; MAKING A COPY OF A BLANK PAGE; TURNING OFF THE POWER FOR 2 MINUTES; REPEATING STEPS FOR SECOND TIME?		
21. ARE THE INSTRUCTIONS POSTED NEAR THE COPIER WHO TO CONTACT IF THERE IS A PAPER JAM OR IF TEXT APPEARS ON COPY OF A BLANK PAGE WHEN SANITIZING?		
22. IS THE U/SO AWARE OF THE APPROVED METHOD FOR SANITIZING COPIER TONER CARTRIDGES?		

SEE NEXT PAGE FOR INSTRUCTIONS

SECURITY REVIEW CHECKLIST FOR FACSIMILE DEVICE/DIGITAL COPIER CERTIFICATION

INSTRUCTIONS

THIS FORM IS PROVIDED TO AID THE OPERATOR IN DOCUMENTING HIS OR HER ASSURANCE THAT THE FAX DEVICE OR DIGITAL COPIER BEING REVIEWED IS CERTIFIABLE AS MEETING ALL THE APPLICABLE IS SECURITY REQUIREMENTS NECESSARY TO PROCESS CLASSIFIED INFORMATION IN A SECURE ENVIRONMENT.

THE CHECKLIST CONTAINS A SERIES OF QUESTIONS, FOR WHICH YES OR NO ANSWERS WILL SUFFICE. THE QUESTIONS IN THE FIRST SECTION APPLY TO FAX DEVICES AND DIGITAL COPIERS. THE QUESTIONS IN THE SECOND SECTION APPLY ONLY TO FAX DEVICES, AND THE QUESTIONS IN THE THIRD SECTION APPLIES ONLY TO DIGITAL COPIERS. EACH QUESTION IN THE APPROPRIATE SECTION MUST BE ANSWERED IN THE AFFIRMATIVE BEFORE THE SECURITY OF THE FAX DEVICE OR DIGITAL COPIER CAN BE CERTIFIED BY THE ISSO TO THE ISSM.

WHEN ALL THE QUESTIONS HAVE BEEN ANSWERED IN THE AFFIRMATIVE, AND THE OPERATOR, THE ISSO AND THE HSO ARE SATISFIED THAT ADEQUATE PROTECTION HAS BEEN PROVIDED FOR THE SECURITY OF THE EQUIPMENT, THE SIGNED AND DATED FORM MUST BE FORWARDED IN A PACKAGE, ALONG WITH THE INDIVIDUAL FACSIMILE DEVICE/DIGITAL COPIER SECURITY PLAN AND OTHER APPLICABLE DOCUMENTATION TO THE ISSM, SO-332/GTN. | REGARDING QUESTION 1, APPLICABLE DOCUMENTATION INCLUDES THE CURRENT, APPROVED DOE HQ MASTER IS SECURITY PLAN FOR FACSIMILE DEVICES AND DIGITAL COPIERS AND COPIES, SIGNED WHERE NECESSARY, OF THE FOLLOWING ATTACHMENTS:

ATTACHMENT 1 - FACSIMILE DEVICE/DIGITAL COPIER U/SO CODE OF CONDUCT |

ATTACHMENT 4 - THIS SECURITY REVIEW CHECKLIST FOR FACSIMILE DEVICE/DIGITAL COPIER CERTIFICATION

ATTACHMENT 5 - INDIVIDUAL FACSIMILE DEVICE/DIGITAL SECURITY PLAN

(THIS PAGE INTENTIONALLY LEFT BLANK)

INDIVIDUAL FACSIMILE DEVICE/DIGITAL COPIER SECURITY PLAN

Please Note: All sections must be completed. Use bond paper for continuation, as required.

SYSTEM ID: HQ-_____(ISSM will Assign) **Date of Plan: ___/___/___**

INITIAL ACCREDITATION					
REACCREDITATION					
DECOMMISSION		ISSO SIGNATURE		EFFECTIVE DATE	

SECTION I. PERSONNEL INFORMATION

	NAME		ORGANIZATION	MAIL STOP	TELEPHONE NUMBER
I-1 HSO					
I-2 ISSO					
I-3 PRIMARY OPERATOR					
I-4 ALTERNATE OPERATOR					
I-5 LOCATION: BUILDING		ROOM NUMBER			

SECTION II. SYSTEM IDENTIFICATION

II-1 EQUIPMENT IDENTIFICATION (Select one): FACSIMILE DEVICE or DIGITAL COPIER:_____

DOE PROPERTY TAG #		MANUFACTURER		MODEL NUMBER	

II-2 EQUIPMENT CONFIGURATION AND FEATURES: (YES, IF PRESENT, NO, IF NOT)

FIXED HARD DISK		REMOVABLE HARD DISK		FACSIMILE		SCANNER		PRINTER	

*** II-3 IS TO BE COMPLETED BY THE O/SO RESPONSIBLE FEDERAL MANAGER, REFER TO PAGE 1-2 OF THE MASTER SECURITY PLAN FOR AN EXPLANATION OF SENSITIVITY LEVELS OF CONCERN**

II-3 SENSITIVITY LEVEL OF CONCERN: (SELECT ONE) HIGH, MEDIUM OR LOW _____

CLASSIFICATION LEVEL: _____ CATEGORY:_____

II-4 SPECIAL HANDLING REQUIREMENTS: NODIST (DEPT OF STATE NO DISTRIBUTION):_____ LIMDIST (LIMITED DISTRIBUTION)_____

EXDIST (EXCLUSIVE DISTRIBUTION):_____ ORCON (ORIGINATOR CONTROLLED):_____

SECTION III. STU (SV/DS) CONNECTION (Not applicable to digital copiers)

III-1. STU-III MANUFACTURER IS:		STU-III TELEPHONE NUMBER:	

SECTION IV. ADDITIONS TO THE DOE HQ MASTER IS SECURITY PLAN FOR FAX DEVICES & DIGITAL COPIERS

IV-1. Statement of Threat:	
IV-2. Risk Assessment:	
IV-3. Contingency Plan:	
IV-4. Comments:	

SECTION V. DEVIATIONS FROM DOE HQ MASTER IS SECURITY PLAN FOR FAX DEVICES & DIGITAL COPIERS

V-1. Master Plan Reference(s):	
V-2. Alternate Procedure(s):	

SECTION VI. FEATURES/FUNCTIONS (Not applicable to digital copiers)

VI-1 ALLOWED (ENABLED) FEATURES/FUNCTIONS:

(1) Clock Adjustment	(12)Programming End Messages
(2) Communicated Page Counter	(13) Programming the ID Code
(3) Department Code On/Off	(14) Programming Remote Terminal ID
(4) Digital Interface Parameter List	(15) Programming Transmit Terminal ID
(5) Edit or Create Digital Interface Mode	(16) Select Date & Time on Reports Control
(6) Load or Delete Digital Interface Mode	(17) Switching Super Smoothing On/Off
(7) Page Count On/Off	(18) Switching Transmit Terminal ID On/Off
(9) Printing a Transaction Confirmation Rpt	(19) Transmission Report On/Off
(10) Printing Number List	(20) Programming DI Mode Password
(11) Scanned & Printed Page Counter	

VI-2 PROHIBITED (DISABLED) FEATURES/FUNCTIONS:

(1) Authorized Reception On/Off	(15) Reception Mode Switching Timer
(2) Clearing Memory Files	(16) Send Later
(3) Clearing Polling Files	(17) Switching Error Correction Mode On/Off
(4) Forwarding On/Off	(18) Telephone Line Type Selection
(5) Printing a Confidential Message	(19) Volume Adjustment
(6) Printing the Authorized Reception List	(20) Multi-copy
(7) Printing the Contents of a Memory File	(21) Polling Transmission/Reception
(8) Printing the Store and Forward FileList	(22) Printing the Polling File List
(9) Programming Authorized Reception	(23) Programming the Quick Dial Characters
(10) Programming the Confidential Password	(24) Programming Quick Dial and Speed Dial
(11) Programming Called Subscriber ID	(25) Switching PSTN Busy On/Off
(12) Programming Groups	(26) Printing Quick Dial Character List
(13) Programming a Forwarding Telephone #	(27) PSTN Mode Enable/Disable
(14) Program Fax Terminal's Telephone #	(28) Printing the Program List

SECTION VII. FEDERAL MANAGERS RISK STATEMENT (TO BE COMPLETED BY THE U/SO'S RESPONSIBLE FEDERAL MANAGER

I HAVE DETERMINED THAT THE U/SO, IDENTIFIED ABOVE, HAS A VALID NEED-TO-KNOW TO PROCESS CLASSIFIED INFORMATION WHICH IS OUTLINED ABOVE (SECTION ii-3). WE ARE AWARE OF OUR SECURITY RESPONSIBILITIES TO SECURELY USE, PROCESS AND PROTECT CLASSIFIED INFORMATION.

RESPONSIBLE FEDERAL MANAGERS NAME	SIGNATURE	DATE

SECTION VIII. CERTIFICATION/ACCREDITATION SIGNATURES

By signing below, the following officials assure a full understanding of their responsibilities as prescribed in the Master IS Security Plan for Facsimile Devices and Digital Copiers, and that the above information is correct.

	PRINTED NAME	SIGNATURE	DATE
VIII-1 U/SO ASSURANCE			
VIII-2 ISSO CERTIFICATION			
VIII-3 HSO CONCURRENCE			
VIII-4 ISSM ACCREDITATION	Bonita S. Agee		

VIII-5 THE SYSTEM REPRESENTED BY THIS PLAN IS ACCREDITED TO PROCESS CLASSIFIED INFORMATION UP TO AND INCLUDING THE LEVEL OF:	ACCREDITATION DURATION NUMBER OF MONTHS

INDIVIDUAL FACSIMILE DEVICE/DIGITAL COPIER SECURITY PLAN
INSTRUCTIONS

The Individual Facsimile Device/Digital Copier Security Plan details specific equipment characteristics, which includes the unique system ID that is assigned by the ISSM. This form assures that the assigned facsimile device or Digital Copier complies with the standard classified guidelines and records personnel, equipment, and interconnection information. Provisions have been included on this plan to document classification levels and percentages of the information sent, received, or copied. Special categories and caveats are also provided, check all that apply. A features/functions section for fax devices provides a place to document which features have been enabled and which have been disabled. Finally, this form records the additions to, and deviations from, the DOE HQ Master IS Security Plan for Facsimile Devices and Digital Copiers, along with signatures of certification and accreditation. It should be noted that the Individual Facsimile Device/Digital Copier Security Plan is used with the Master IS Security Plan and it is not used to gain accreditation to process classified information in and of itself.

This form is divided into seven sections.

Section I--Personnel Information: This first section, Personnel Information, is self-explanatory and includes the name, organization, mail stop, and telephone number of the ISSO, HSO, the Primary Operator, or Key Operator and the Alternate Operator.

I-5--Location: Enter the building and room where the Facsimile Device or Digital Copier is installed.

Section II--System Identification: The second section, System Identification, includes the classification levels and amounts, a description of the Facsimile Device or Digital Copier, and Special handling categories.

Section III--STU-III Connection: This brief section requests information on the STU-III used with the facsimile Device.

Section IV--Additions to the Master Plan: This section is devoted to the compliance of the system to the DOE HQ Master IS Security Plan for Fax Devices and Digital Copiers. This section should describe any additional safeguards implemented in the Facsimile Device or Digital Copier that do not appear in the Master Plan.

Section V--Deviations from the Master Plan: This section is devoted to any ways in which the safeguards implemented in the individual Facsimile Device or Digital Copier deviate from those described in the Master IS Security Plan for Fax Devices and Digital Copiers. Any deviations must be listed and alternative methods of protection described.

Section VI--Operating Modes/Features/Functions: This section applies to Fax Devices only and documents how the device is used, which features are enabled and which features are disabled.

SECTION VII--Managers Acceptance of Risk Statement and Signature: This section provides the managers approval for the user to process classified.

Section VIII--Certification/Accreditation Signatures: This section provides a place for each security official to certify compliance with the DOE Classified Computer Security Program and that safeguards are implemented to protect classified document transmissions on the Facsimile Device or reproduced on the Digital Copier.

(THIS PAGE INTENTIONALLY LEFT BLANK)